

Semiquantum key distribution using entangled states

Jian Wang¹, Sheng Zhang, Quan Zhang, Chao-Jing Tang

School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China

Abstract

Recently, Boyer et al. presented a novel semiquantum key distribution protocol [M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. 99, 140501 (2007)], by using four quantum states, each of which is randomly prepared by Z basis or X basis. Here we present a semiquantum key distribution protocol by using entangled states in which quantum Alice shares a secret key with classical Bob. We also show the protocol is secure against eavesdropping.

Keywords: semiquantum key distribution; entangled state

PACS: 03.67.Dd; 03.67.Hk

1. Introduction

Quantum key distribution (QKD) is one of the most promising applications of quantum information science. The goal of QKD is to allow two legitimate parties, Alice and Bob, to generate a secret key over a long distance, in the presence of an eavesdropper, Eve, who interferes with the signals. The security of QKD is based on the fundamental laws of physics. Since the BB84 protocol[1], the first QKD scheme, was published, many variations on QKD have been subsequently proposed. They can be roughly classified into “prepare and measure” protocols, such as BB84, B92[2], the three-state protocol[3], the six-state protocol[4] and “entanglement based” protocols, such as E91[5], BBM92[6]. There have been efforts made to set a security proof based on entanglement for the both classes[7].

QKD protocols claim that both the parties are quantum. That is to say, both parties should perform quantum operation on their qubits. Boyer et al. considered a new problem that in the QKD protocol if one party is quantum and the other has only classical capabilities, whether the protocol could achieve to distribute a key between the parties securely. They then presented a novel semiquantum key distribution protocol[8] (hereafter called BKM07 protocol), in which one party (Alice) is quantum and the other (Bob) is classical, and proved that the protocol is completely robust against an eavesdropping attempt. Similar to BB84, in their protocol, Alice prepares a random qubit in the computational (Z) basis $\{|0\rangle, |1\rangle\}$ or Hadamard (X) basis $\{|+\rangle, |-\rangle\}$ and sends it to Bob. They call the computational basis classical and use the classical notion $\{0, 1\}$ to describe the two quantum states $\{|0\rangle, |1\rangle\}$. Bob can access a segment of the quantum channel, but he is restricted to performing some classical operations. Different from BB84, he can only measure the transmission qubits in the classical $\{0, 1\}$ basis, prepare a qubit in the classical basis

¹Tel. No.: 86 0731 84575706, E-mail address: jwang@nudt.edu.cn

and send it, reflect it to Alice directly or reorder the qubits (for example, by using different delay lines). As Bob can only deal with qubits in the classical basis, he is regarded as a classical party.

To ensure the security of BKM07 protocol, the communication parties should keep Eve from knowing which is a particle that Bob measured in the computational basis and which is a particle that Bob reflected to Alice directly. Actually, BKM07 protocol is similar to BB84 protocol if we regard Bob as the initiator in BKM07 protocol. Bob selects randomly either to measure the receiving qubit and resend it or reflect it directly, which looks like Bob prepares randomly the four quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Boyer et al. showed a different semiquantum key distribution protocol[9] based on randomization (hereafter called BGKM09-Randomization-based protocol). Different from BKM07 protocol, Bob can reorder the particles besides measuring and preparing a qubit in the classical basis in BGKM09-Randomization-based protocol. In order to avoid Eve's acquiring Bob's operation information on each receiving qubit, Bob reorders randomly the reflected qubits. Furthermore, they proved the robustness of the protocol in much more general scenario. Zou et al. presented five different semiquantum key distribution protocols[10] in which Alice sends three quantum states, two quantum states and one quantum state, respectively. Li et al. proposed two semiquantum secret sharing protocols[11] by using maximally entangled Greenberger-Horne-Zeilinger states in which quantum Alice shares a secret with two classical parties, Bob and Charlie.

In this Letter, we present a semiquantum key distribution protocol by using entangled states. We follow the descriptions about classical in Ref.[8]. Quantum Alice can prepare two-particle entangled states and measure the particles in Bell basis or computational basis. Classical Bob is restricted to measuring, preparing, reordering, or sending quantum states only in the fixed orthogonal quantum basis set $\{|0\rangle, |1\rangle\}$. We show that Eve's eavesdropping would inevitably disturb the transmission quantum states and the communication parties could detect Eve's attack.

2. Description of the protocol

We then describe the semiquantum key distribution protocol using entangled states in detail. Suppose Alice wants to share a secret key with classical Bob. The protocol comprises the following steps.

- (1) Alice prepares N Bell states, each of which is in the state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}, \quad (1)$$

where A, B represent the two particles of each state. Alice takes one particle from each state to form an ordered partner particle sequence $[B_1, B_2, \dots, B_N]$, called B particle sequence. She then send the N particles $[B_1, B_2, \dots, B_N]$ to Bob.

- (2) For each particle arriving, Bob selects randomly either to measure it in the computational basis (SIFT it) or to reflect it to Alice directly (CTRL it). Bob reorders randomly the N particles and generates a rearranged particle sequence $[B'_1, B'_2, \dots, B'_N]$, called B' particle sequence. He then sends B' particle sequence to Alice. The order of the rearranged particle sequence is completely secret to others but Bob himself, which ensures the security of the present scheme.

- (3) Alice stores the receiving particles in quantum memory and informs Bob that she has received the N particles. Bob publishes which particles he chose to CTRL and the secret rearranged order of the particle sequence.

- (4) For each of the CTRL particles (those were reflected directly), Alice performs Bell basis measurement on the reflected particle B and particle A she owned. If there is no eavesdropping,

Alice's measurement result should be $|\phi^+\rangle$. Alice analyzes the error rate on the CTRL particles according to her measurement results. If the error rate is higher than the threshold they preset, they abort the protocol. We call this step the first eavesdropping check.

(5) For each of the SIFT particles (those were measured in the computational basis), Alice performs Z basis measurement on particle A and particle B. She chooses randomly a sufficiently large subset from the measurement results for eavesdropping check. She announces which are the chosen particles. Bob then publishes his measurement results. Alice checks the error rate and if it is below the threshold they preset, they proceed to execute the next step. Otherwise they abort the protocol. We call this step the second eavesdropping check.

(6) Alice announces error correction code (ECC) and privacy amplification (PA) data. Alice and Bob utilize the ECC and PA to extract the final key.

Obviously, the protocol can also be realized by using some other entangled states, such as $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}$, $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}$ and $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}$. Similar to BKM07 protocol, Bob can make use of a different sifting method called measure-resend at step (2). We only need to modify step (2)-(3) of the previous protocol. The modified steps are as follows:

(2') For each particle arriving, Bob selects randomly either to measure it in the computational basis and resend it to Alice after measurement (SIFT it) or to reflect it to Alice directly (CTRL it).

(3') Alice stores the receiving particles in quantum memory and informs Bob that she has received the N particles. Bob publishes which particles he chose to SIFT and which particles he reflected directly to Alice.

We call the modified protocol measure-resend protocol. In the measure-resend protocol, Bob only needs to perform computational basis measurement on the particles and reflect the particles directly.

3. The security for the protocol

The key of the security of the protocol is to keep Eve from knowing which particles are CTRL particles and which ones are SIFT particles. If Eve can distinguish CTRL and SIFT particles properly, she can easily achieve the secret key by performing computational basis measurements on the SIFT particles. At step (2) of the protocol, Bob reorders the particles so that no one could distinguish CTRL and SIFT particles properly except Bob. However, Eve can distinguish Bob's operation properly with a certain probability in the measure-resend protocol. Of course, Eve's eavesdropping will be detected by communication parties during the second eavesdropping check. Suppose Eve intercepts particle B at step (1) and prepares a Bell state $|\phi^+\rangle_{EE'} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{EE'}$. She sends particle E' to Bob instead of particle B and keeps particle E . She reflects particle B directly to Alice without disturbing it. According to step (2'), Bob chooses randomly either to SIFT it or to CTRL it. If Bob chooses to SIFT, $|\phi^+\rangle_{EE'}$ will collapse to $|00\rangle_{EE'} = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle)_{EE'}$ or $|11\rangle_{EE'} = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle)_{EE'}$ each with probability of 1/2. If Bob chooses to CTRL, $|\phi^+\rangle_{EE'}$ keeps unchanged. After Bob sending particle E' to Alice, Eve intercepts particle E' and performs Bell basis measurement on particle E and E' . If she obtains $|\phi^-\rangle$, she can ascertain that Bob has chosen to SIFT. If Bob chooses to SIFT or CTRL each with probability of 1/2, Eve can acquire his operation information properly with probability of 1/4. The communication parties cannot detect the exist of Eve during the first eavesdropping check. However, Eve's attack cannot escape from the second eavesdropping check. We'd best not let

Eve have a chance of distinguishing CTRL and SIFT particles properly. For the protocol using order rearrangement, this trick of Eve's will inevitably fail.

According to Stinespring dilation theorem[12], the attack of an eavesdropper Eve can be realized by a unitary operation \hat{E} on a large Hilbert space, $H_{AB} \otimes H_E$. Then the state of Alice, Bob and Eve is

$$|\Phi\rangle = \sum_{a,b \in \{0,1\}} |\varepsilon_{a,b}\rangle |a\rangle |b\rangle, \quad (2)$$

where $|\varepsilon\rangle$ denotes Eve's probe state. $|a\rangle$ and $|b\rangle$ are states shared by Alice and Bob. The condition on the states of Eve's probe is

$$\sum_{a,b \in \{0,1\}} \langle \varepsilon_{a,b} | \varepsilon_{a,b} \rangle = 1. \quad (3)$$

We can describe Eve's attack on the system as

$$\hat{E}|0, \varepsilon\rangle = \alpha|0, \varepsilon_{00}\rangle + \beta|1, \varepsilon_{01}\rangle, \quad (4)$$

$$\hat{E}|1, \varepsilon\rangle = \beta'|0, \varepsilon_{10}\rangle + \alpha'|1, \varepsilon_{11}\rangle, \quad (5)$$

where $|\alpha|^2 + |\beta|^2 = 1, |\beta'|^2 + |\alpha'|^2 = 1$. Eve can eavesdrop particle B at step (1) and the state of composite system will be

$$\begin{aligned} |\Phi\rangle &= \frac{1}{\sqrt{2}} [|0\rangle_A (\alpha|0, \varepsilon_{00}\rangle + \beta|1, \varepsilon_{01}\rangle)_{BE} + |1\rangle_A (\beta'|0, \varepsilon_{10}\rangle + \alpha'|1, \varepsilon_{11}\rangle)_{BE}] \\ &= \frac{1}{\sqrt{2}} [\alpha|0, 0, \varepsilon_{00}\rangle + \beta|0, 1, \varepsilon_{01}\rangle + \beta'|1, 0, \varepsilon_{10}\rangle + \alpha'|1, 1, \varepsilon_{11}\rangle]_{ABE} \\ &= \frac{1}{\sqrt{2}} [(\alpha|0, \varepsilon_{00}\rangle + \beta'|1, \varepsilon_{10}\rangle)_{AE} |0\rangle_B + (\beta|0, \varepsilon_{01}\rangle + \alpha'|1, \varepsilon_{11}\rangle)_{AE} |1\rangle_B]. \end{aligned} \quad (6)$$

If Bob chooses to SIFT, $|\Phi\rangle$ will collapse to $(\alpha|0, \varepsilon_{00}\rangle + \beta'|1, \varepsilon_{10}\rangle)_{AE} |0\rangle_B$ or $(\beta|0, \varepsilon_{01}\rangle + \alpha'|1, \varepsilon_{11}\rangle)_{AE} |1\rangle_B$ each with probability of 1/2. In the course of the communication parties' checking the errors on the SIFT particles at step (5), the error rate introduced by Eve is $e = |\beta|^2 = |\beta'|^2 = 1 - |\alpha|^2 = 1 - |\alpha'|^2$. If Bob chooses to CTRL, particle B will be reflected directly. Eve can intercept particle B again and perform another unitary operation \hat{E}' on $|\Phi\rangle$, the state of the system becomes

$$\begin{aligned} |\Phi'\rangle &= \frac{1}{\sqrt{2}} [\gamma|0, 0, \varepsilon'_{00}\rangle + \delta|0, 1, \varepsilon'_{01}\rangle + \delta'|1, 0, \varepsilon'_{10}\rangle + \gamma'|1, 1, \varepsilon'_{11}\rangle]_{ABE} \\ &= \frac{1}{2} [\gamma(|\phi^+\rangle + |\phi^-\rangle)_{AB} |\varepsilon'_{00}\rangle_E + \delta(|\psi^+\rangle + |\psi^-\rangle)_{AB} |\varepsilon'_{01}\rangle_E \\ &\quad + \delta'(|\psi^+\rangle - |\psi^-\rangle)_{AB} |\varepsilon'_{10}\rangle_E + \gamma'(|\phi^+\rangle - |\phi^-\rangle)_{AB} |\varepsilon'_{11}\rangle_E]. \end{aligned} \quad (7)$$

When the communication parties check the errors on the CTRL particles at step (4), the error rate introduced by Eve is $e = 1 - (|\gamma|^2 + |\gamma'|^2)/4$. If Eve attempts to obtain information, she would inevitably induce some errors that legitimate parties could notice.

To explain the error rate introduced by Eve, we take an example for individual attack strategy. Suppose Eve intercepts the particles in B particle sequence transmitted to Bob at step (1) and

makes measurements on them. She then resends particles to Bob according to her measurement results. In this way, if Eve measures particle B in the Z basis, $|\phi^+\rangle$ will collapse to $|00\rangle_{AB}$ or $|11\rangle_{AB}$. If Eve's result is $|0\rangle$ ($|1\rangle$), she sends a particle in the state $|0\rangle$ ($|1\rangle$) to Bob. According to the protocol, Bob chooses randomly either to SIFT it or to CTRL it and reorders the particles. Because $|00\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle)$ ($|11\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle)$), during the first eavesdropping check, Alice performs Bell basis measurement on particle A and B, and obtains $|\phi^+\rangle$ or $|\phi^-\rangle$ each with probability of 1/2. Thus the error rate introduced by Eve is 50%. Suppose Eve intercepts particle B at step (1) and uses it and her own ancillary particle in the state $|0\rangle$ to do a CNOT operation (particle B is the controller, Eve's ancillary particle is the target). Eve then resends particle B to Bob. The state of particle A, B and Eve's ancillary particle becomes $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABE}$. At step (2), Bob selects randomly either to SIFT or to CTRL and reorders the particles. In view of $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABE} = \frac{1}{2}[(|\phi^+\rangle + |\phi^-\rangle)|0\rangle + (|\phi^+\rangle - |\phi^-\rangle)|1\rangle]$, Alice obtains $|\phi^+\rangle$ or $|\phi^-\rangle$ each with probability of 1/2 at step (4). Thus the error rate introduced by Eve will reach 50% and her eavesdropping will be detected.

4. Conclusion

So far we have proposed a semiquantum key distribution protocol by using entangled states and analyzed the security for the present protocol. In the protocol, quantum Alice can share a secret key with classical Bob. Bob is restricted to measuring a particle in the classical basis, preparing a particle in the classical basis, reflecting a particle directly, or reordering the particles. Bob utilizes order rearrangement to keep Eve from distinguishing which particles Bob chose to CTRL and which particles he chose to SIFT. The communication parties make use of twice eavesdropping checks to ensure the security of the protocol. Since the users only need to perform some classical operations on particles, semiquantum key distribution can be realized at a low cost. It also provides a good idea for building quantum key distribution network (For example, we can build a Key Distribution Center which is quantum, but the users have only classical capabilities). There are many difficulties to be dealt with when implementing semiquantum key distribution in the practical scenario. We would like to explore these problems in future.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 60872052.

References

- [1] C. H. Bennett, G. Brassard, in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179.
- [2] C. H. Bennett, Phys. Rev. Lett. 68 (1992) 3121.
- [3] H. Bechmann-Pasquinucci, A. Peres, Phys. Rev. Lett. 85 (2000) 3313.
- [4] D. Bruss, Phys. Rev. Lett. 81 (1998) 3018.
- [5] A. K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
- [6] C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. 68 (1992) 557.
- [7] M. Curty, M. Lewenstein, N. Lutkenhaus, Phys. Rev. Lett. 92 (2004) 217903.
- [8] M. Boyer, D. Kenigsberg, T. Mor, Phys. Rev. Lett. 99 (2007) 140501.
- [9] M. Boyer, R. Gelles, D. Kenigsberg, T. Mor, Phys. Rev. A 79 (2009) 032341.

- [10] X. Zou, D. Qiu, L. Li, L. Wu, L. Li, Phys. Rev. A 79 (2009) 052312.
- [11] Q. Li, W. H. Chan, D. Y. Long, Phys. Rev. A 82 (2010) 022303.
- [12] W. F. Stinespring, Proc. Am. Math. Soc. 6 (1955) 211.